Express Mail Label No.: EV308899013US
Date of Deposit: October 31, 2003

INDUSTRIAL OR DOMESTIC LOCAL NETWORK

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to a local network of industrial or domestic type intended for the control and/or the supervision of various appliances by means of one or several distributed (or delocalized) computers.

Discussion of the Related Art

Fig. 1 very schematically illustrates the architecture of an industrial or domestic network. Network N enables connection of several devices, three devices D_1, D_2, D_3 being shown in Fig. 1. Each device is for example formed of a computer, of an actuator controlled by a microprocessor or of a sensor connected to a microprocessor. Each device D_1, D_2, D_3 comprises an application system A_1, A_2, A_3 and a communication circuit C_1, C_2, C_3. Communication circuit C_1, C_2, C_3 may comprise a microprocessor or a programmable logic and ensures the reception and the transmission of information frames over network N. Application system A_1, A_2, A_3 comprises a microprocessor or a programmable logic which, under control of a program that may be modified by a user, processes the information frames transmitted and received by communication circuit C_1, C_2, C_3. Application system A_1, A_2, A_3 may further be connected to actuators or

sensors. Application system A_1, A_2, A_3 and communication circuit C_1, C_2, C_3 may be formed by separate integrated circuits connected by wire links W.

Generally, application system A_1, A_2, A_3 sets up the information frames sent to communication circuit C_1, C_2, C_3 according to operating parameters of network N so that they can be properly transmitted over network N by communication circuit C_1, C_2, C_3. The network operating parameters are the set of parameters which define the data flows over the network, the priorities between the devices connected to the network, the shape of the information frames transmitted over the network, etc. The information frames may also be directly set up by communication circuit C_1, C_2, C_3 according to the network operating parameters which are set by application system A_1, A_2, A_3 and which can be modified by it.

A disadvantage is that by modifying the elements forming application system A_1, A_2, A_3 of a device D_1, D_2, D_3 connected to network N, for example, by modifying the program executed by the microprocessor of application system A_1, A_2, A_3, it is possible to modify the network operating parameters used by device D_1, D_2, D_3 and thus to alter, or even to interrupt the operation of network N. It may then be difficult to find out the origin of the anomaly and to correct it, and the network may be definitely deteriorated. Similarly, when a new device is connected to network N, it is assumed that the application system of the new device has network operating parameters which are adapted to the network N to which the device is connected. In the case where such parameters are incorrect, the new device connected to network N can alter, or even interrupt, the general operation of network N.

Summary of the invention

The present invention aims at a secure exchange of information frames over a local network which limits risks of alteration of the network operation by one of the devices connected to the network.

For this purpose, it provides a method for exchanging information frames over a network between devices, each device comprising a communication circuit connected to a processing unit and comprising addresses, each address being associated with a transmission or reception indicator, a single device comprising a same address associated with a transmission indicator, in which each address is associated with a memory containing an information frame that can be modified and/or read by the processing unit, and comprising the steps of having a master device periodically transmit addresses; having the communication circuit of the device for which the address transmitted by the master device is associated with a transmission indicator transmit the information frame contained in the memory associated with said address and provide the processing unit with an identifier of said address; and having each communication circuit of a device for which the address transmitted by the master device is associated with a reception indicator write into the memory associated with said address of said information frame and provide the processing unit with an identifier of said address.

According to an embodiment of the present invention, the processing units, except for the processing unit of the master device, can neither read nor modify the addresses and the transmission and/or reception indicators of the communication circuits to which they are connected.

According to an embodiment of the present invention, all communication circuits further comprise a first address identical for all devices and associated with a transmission indicator and a second address identical for all devices and associated with a reception indicator, the connection of a new device to the network comprising the steps of having the master device periodically transmit the first address; having the communication circuit of the new device, upon reception of the first address, transmit an identification frame; having the master device successively transmit the second address and a

parameterizing frame defined based on the identification frame; having the communication circuit of the new device, upon successive reception of the second address and of the parameterizing frame, modify its addresses and reception and/or transmission indicators based on the parameterizing frame.

According to an embodiment of the present invention, each device comprises a specific identification number stored in the communication circuit, the identification frame transmitted by the communication circuit of the new device comprising the specific identification number of said new device, the parameterizing frame transmitted by the master device comprising the specific identification number of said new device.

According to an embodiment of the present invention, the communication circuit of the new device transmits no data as long as it has not received the first address.

According to an embodiment of the present invention, the communication circuit of each device comprises a privilege indicator at a first value when the device is likely to transmit addresses over the network and at a second value otherwise, said privilege indicator being set to the first or to the second value by the communication circuit of the new device based on the parameterizing frame.

The present invention also provides a device intended to be connected to a network comprising a communication circuit and connected to a processing unit, comprising an address table, a register table, each register in the register table being associated with an address in the address table and a direction table comprising one direction indicator per address, said processing unit being capable of reading information frames stored in the registers or writing information frames into the registers, said communication circuit being capable, upon reception of a request received from the network and corresponding to one of said addresses, of transmitting over the network the information frame stored in the register associated with said address if the corresponding direction indicator is of

a first determined type, or of writing an information frame received from the network into the register associated with said address if the corresponding direction indicator is of a second determined type, and being capable of transmitting to the processing unit an identifier of the register associated with said address.

According to an embodiment of the present invention, the address table comprises a first address identical for all the devices connected to the network, the direction table comprising a direction indicator associated with said first address of the first type, the communication circuit of the device being adapted to transmitting said addresses and the associated direction indicators over the network upon reception of said first address.

According to an embodiment of the present invention, the address table comprises a second address identical for all circuits connected to the network, the direction table comprising a direction indicator associated with said second address of the second type, and being capable, upon successive reception of the second address and of a parameterizing frame, of modifying the addresses and the associated direction indicators based on the parameterizing frame.

The foregoing object, features, and advantages of the present invention will be discussed in detail in the following non-limiting description of specific embodiments in connection with the accompanying drawings.

Brief Description of the Drawings

Fig. 1, previously described, illustrates an example of a conventional local network;

Fig. 2 shows the characteristic operating parameters used by a slave device according to the present invention connected to the network;

Fig. 3 shows the characteristic operating parameters used by a master device according to the present invention connected to the network; and

Fig. 4 schematically shows an example of implementation of the method of information frame exchange between a master device of the network and a new device connected to the network.

Detailed Description

The present invention consists, for most devices connected to the network and called slave devices, of limiting the data likely to be exchanged between the application system and the communication system of the device, so that the application system has no access to the network operating parameters used by the communication circuit to exchange information frames over the network. The application system of a slave device thus cannot modify the network operating parameters, whatever the modifications brought to the application system, for example at the level of the program executed by the application system's microprocessor. A single device connected to the network and called the master device has the ability to modify the network operating parameters used by the slave devices.

Fig. 2 shows an example of the forming of a slave device D according to the present invention comprising an application system A connected to a communication circuit C, communication circuit C being capable of exchanging information frames over a network N. According to the type of network N, devices D may all be connected to a bus or be interconnected by point-to-point links. Communication circuit C comprises a communication unit P_C capable of exchanging information frames with network N according to parameters stored in memories. Application system A comprises a processing unit P_A capable of receiving data provided by communication unit P_C and of processing data stored in a memory, for example, by executing a program.

Communication circuit C comprises an address table (Address) in which are stored addresses X_1 to X_{J+2}, where J is the number of simultaneous communication channels that a device D may have with other devices connected to network N. Each address X_1 to X_J is associated with a single communication

channel. Value J varies according to the type of device D connected to network N. The address table may comprise only certain addresses from among addresses X_1 to X_J and the cells of the address table unused by device D are placed at an arbitrary inhibition value. Addresses X_{J+1} and X_{J+2} are always present for all devices D connected to network N. Addresses X_1 to X_{J+2} may correspond to binary data, for example, of 16 bits. To address X_{J+1} corresponds a specific information frame, called the parameterizing frame (CS_Reception), which is stored at the level of communication channel C. To address X_{J+2} corresponds a specific information frame called the identification frame (CS_Transmission), stored at the level of the communication circuit. The communication circuit also comprises a direction table (Direction) in which are stored direction indicators, each direction indicator corresponding to a single bit. Each address X_1 to X_{J+2} is associated with a direction indicator which is at 1 or at 0 for addresses X_1 to X_J, at 0 for address X_{J+1} and at 1 for address X_{J+2}. For a given address X_1 to X_J, a single device of the network comprises a direction indicator associated with said address at 1. An identification number U (Unique Number U), specific to each device D likely to be connected to network N, and a privilege indicator (Privilege Bit P) are stored in a memory of communication circuit C. As an example, specific identification number U comprises 63 bits and the privilege indicator comprises a single bit.

Application system A comprises a table (Data) of registers R_1 or R_J in which are stored data that can be of variable size, each register R_1 to R_J being associated with an address X_1 to X_J in the address table.

The data stored in registers R_1 to R_J may be read or modified by communication unit P_C of communication circuit C and by processing unit P_A of application system A. Communication unit P_C may, under certain conditions, modify the different addresses X_1 to X_J, the direction indicators, and privilege indicator P. Processing unit P_A can neither read, nor modify

addresses X_1 to X_J, the direction indicators, and privilege indicator P. Specific identification number U is a characteristic of device D and can be modified neither by communication unit P_C nor by processing unit P_A. Similarly, addresses X_{J+1} and X_{J+2} are characteristics of device D and can be modified neither by communication unit P_C, nor by processing unit P_A. Communication unit P_C is adapted to transmitting to processing unit P_A an identifier I indicating one of registers R_1 to R_J of the register table.

Fig. 3 shows the structure of master device M, which is similar to that shown in Fig. 2. However, conversely to all slave devices, processing unit P_A of application system A of master device M can directly modify the address and direction tables stored at the level of the communication circuit C of master device M. Communication circuit C further comprises a register (Request) where requests Q to be transmitted over network N are successively written by application system A.

The method according to the present invention of information frame exchange over network N is the following. At a given time, only master device M has the possibility to transmit requests Q over network N. Requests Q are received by all the slave devices D connected to network N. Based on a received request Q, each communication unit P_C may determine a same address X_K from among addresses X_1 to X_{J+2}. In particular, request Q may be equal to address X_K.

For each slave device, if address X_K determined based on a received request corresponds to one of stored addresses X_1 to X_J, communication unit P_C determines whether the direction indicator associated with address X_K is at 0 or at 1.

If the direction indicator is at 1, communication unit P_C reads the information frame stored in the data register R_K associated with address X_K and transmits it over network N. Communication unit P_C then sends to processing unit P_A the identifier I associated with the register R_K which has been read

from, to indicate thereto that the information frame stored in register R_K has been transmitted over network N.

If the direction indicator associated with address X_K is at 0, communication circuit C waits to receive an information frame from network N. According to the exchange protocol used by the network, the expected information frame may correspond to the first information frame received by device D after reception of the request or to a subsequent frame. Communication unit P_C then memorizes the received information frame in the data register R_K associated with address X_K, then transmits to processing unit P_A the identifier I associated with register R_K to notify application system A that a new information frame has been stored in the register R_K corresponding to identifier I.

Master device M can also transmit information frames over the network. Indeed, upon transmission of a request Q by master device M, master device M, like the slave devices, receives request Q that it has just transmitted. It is then enough for the direction indicator associated with the address of the transmitted request to be at 1 for master device M to then transmit the information frame stored in the data register associated with the request address.

According to the address and direction tables of the devices connected to the network, data flows may then be established between devices. The address and direction tables thus form the network operating parameters according to the present invention.

For the slave devices connected to the network, processing unit P_A of application system A of each slave device has access neither to the address and direction tables, nor to the privilege indicator of communication circuit C. The application system thus cannot modify the network operating parameters and thus disturb the operation of network N. Only the processing unit of the application system of the master device can directly modify the tables stored in the communication circuit of the master device. However, the operation of the master device being

generally well known, the cause of a malfunction of the network can easily be diagnosed.

Fig. 4 shows an example of successive exchanges of information frames over network N between a master device M and a new device D′ connected to network N.

The new device D′ connected to network N has the architecture shown in Fig. 2. It thus comprises an address table, a direction table, a specific identification number U, and a privilege indicator P. According to the method of the present invention, the new device D′ connected to network N transmits no information frame as long as it has not received an appropriate request transmitted by master device M.

For all the devices connected to network N, the direction indicators associated with addresses X_{J+1} and X_{J+2} are respectively at 0 and 1. The values of addresses X_{J+1} and X_{J+2} are for example FFFF and FFFE. Identification frame CS_Transmission associated with address X_{J+2} especially comprises the set of addresses X_1 to X_J, the direction indicators associated with addresses X_1 to X_J, specific identification number U, and privilege indicator P.

At step 10, master device M transmits over network N a request $Q(X_{J+2})$ associated with address X_{J+2}. Such a request may be periodically transmitted.

At step 12, the new device D′ and all the other devices already connected to network N receive request $Q(X_{J+2})$.

At step 14, the direction indicator associated with address X_{J+2} being at 1, new device D′ transmits identification frame CS_Transmission associated with address X_{J+2}.

At step 16, master device M receives frame CS_Transmission. The connection of a new device D′ to network N is thus known by master device M, which determines based on frame CS_Transmission the address and direction tables and the value of the privilege indicator P of new device D′.

At step 18, master device M transmits a request $Q(X_{J+1})$ associated with address X_{J+1}.

At step 20, new device D′ receives request $Q(X_{J+1})$. The direction indicator associated with address X_{J+1} being at zero, new device D′ starts waiting for an information frame coming from network N.

At step 22, master device M transmits a parameterizing frame CS_Reception that comprises an address table X_1 to X_J, a direction table, a privilege indicator value P, and which recalls the specific identification number U associated with new device D′. The tables and the privilege indicator may be modified with respect to the original values provided by identification frame CS_Transmission.

At step 24, new device D′ and all the devices already connected to the network receive parameterizing frame CS_Reception. Only the communication unit P_C of new device D′ recognizes the specific identification number U present in frame CS_Reception. The address and direction tables and the privilege indicator of this new device are then modified according to the received frame CS_Reception. All the other devices already connected to the network and which also receive frame CS_Reception perform no action, since they do not recognize the specific identification number present in frame CS_Reception as being theirs. New device D′ then inhibits address X_{J+2} to no longer transmit an identification frame CS_Transmission if it subsequently receives a request $Q(X_{J+2})$ associated with address X_{J+2}. New device D′ can then operate normally and transmit over network N information frames upon reception of requests from master device M. The present invention enables configuring a single new device D′ at a time. Indeed, the duration of the configuration being very short, on the order of one microsecond, it is in practice impossible, on keying, to simultaneously connect two new devices on the network.

The privilege indicator P of a new device D′ connected to the network is at 1 when new device D′ has the possibility of behaving, under given conditions, as a master device, that is, of transmitting requests over network N. It may be useful for a

slave device to have the possibility of becoming a master device, especially to overcome a deficiency of the active master device. When at step 16, master device M receives identification frame CS_Transmission and determines the value of privilege indicator P or new device D', it may decide to set the privilege indicator to 0 if it considers that the new device D' must not be able to operate as a master device or to leave the privilege indicator at 1 if it considers that, in certain operating cases, new device D' could be led to operate as a master device.

The present invention has many advantages.

First, it enables application systems of devices to exchange data over a network without knowing the network operating parameters. Indeed, the network operating parameters, which define the data flows between the devices connected to the network, are transmitted by the master device to each new device connected to the network.

Second, it enables rapidly detecting that a new device connected to the network operates "abnormally" in that the new device does not follow the data exchange process according to the present invention. Indeed, a new device according to the present invention connected to the network transmits no information frame as long as it has not received an appropriate request. A new "abnormally"-operating device connected to the network will probably transmit over the network from as soon as it is connected requests or information frames. There then immediately is a conflict between the master device and the new device. The transmission over the network of unwanted requests or information frames very rapidly causes a disturbance of the operation of the other devices connected to the network. Such a disturbance may generally be rapidly acknowledged by an exterior observer and the new device can then be removed from the network.

Third, a new device connected to the network must necessarily notify its presence by transmitting, responsive to a request of the master device, identification frame

CS_Transmission. The master device may then modify the address tables of all the other devices already connected to the network to take into account the presence of the new device connected to the network. The method according to the present invention thus enables avoiding for a new device connected to the network to be "dormant", that is, to transmit no information frame over the network after its connection. The present method thus gives notice of the "awakening" of such a "dormant" device after an undetermined time, such an awakening up being likely to cause an alteration of the network operation, the cause of which could then be difficult to determine.

Fourth, the requests transmitted by the master device over the network may be formed of the mere addresses X_1 to X_{J+2}, which are for example formed of 16 bits. The size of the data transmitted over the network which are necessary to a proper network operation, but that thus contain no "useful" information, that is, information used by the application systems of the devices connected to the network, is thus limited.

Fifth, the communication unit of the communication circuit of the device can be formed with a simple logic gate architecture without requiring a microprocessor or a memory.

Sixth, it enables gathering the network operating parameters in a single location, for example, the master device, and thus enables global administration of the network from a central point.

Of course, the present invention is likely to have various alterations, modifications, and improvements which will readily occur to those skilled in the art. Such alterations, modifications, and improvements are intended to be part of this disclosure, and are intended to be within the spirit and the scope of the present invention. Accordingly, the foregoing description is by way of example only and is not intended to be limiting. The present invention is limited only as defined in the following claims and the equivalents thereto.